100

	WLAN (adhoc)	Bluetooth	FEEL	DECT	Smart-Its Friends	Invention
secure?	yes	yes	yes	yes[1]	not specified	yes
easy-to-use: which user interaction is needed in the best case	entering a name and a key	entering a key	moving two devices together	select from a list & entering a key	do the same action to two devices	press a button at two devices
multiple networks supported?	yes	yes	yes	yes (multiple base stations)	yes	yes
low probability of unwanted registration?	yes	yes	no	yes	despends on the used actions	yes
required additonal hardware means	entering strings	entering strings	none	selection from a text list, entering strings	context sensors	AV,buttons
self-contained registration for which device types?	>=mobile phones	>=mobile phones	mobile devices only	>=mobile phones	yes(but depends on the used actions)	all

[1] If the PIN is the factory default value, an attacker can register with the base station during the 20s period starting when the "Paging" button is pressed. During this time, an attacker could also mask as a base station.
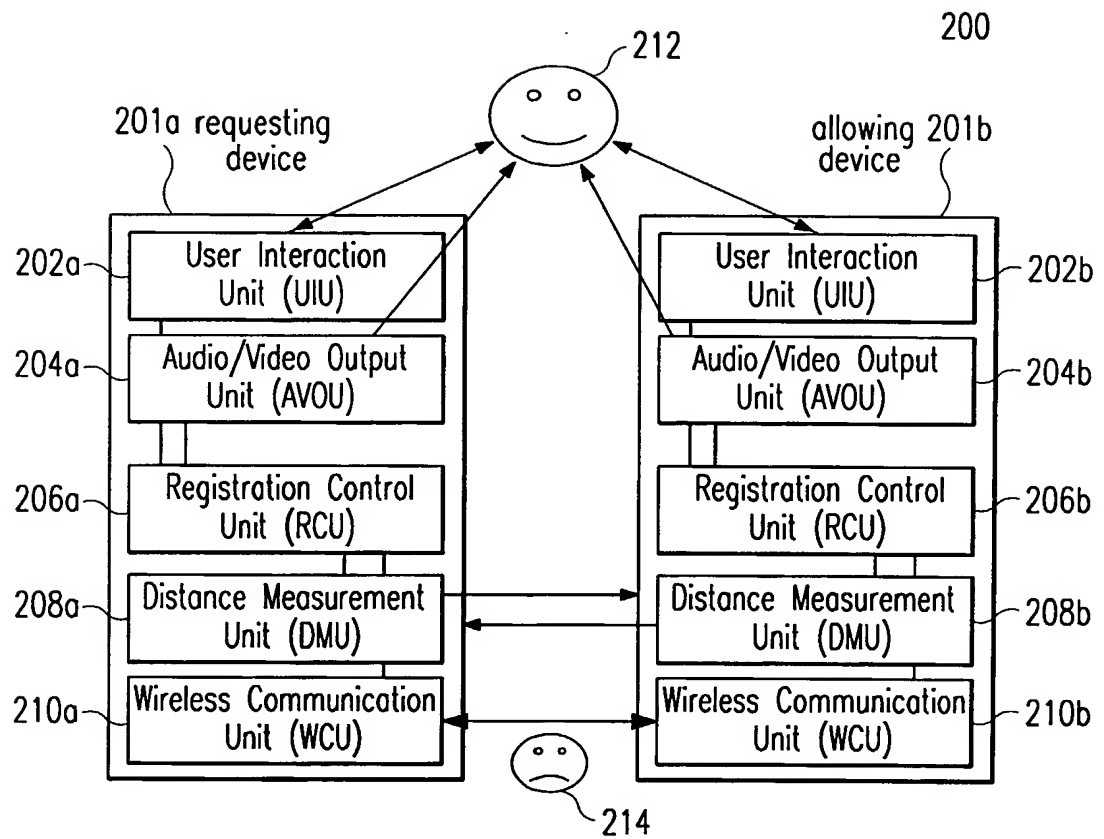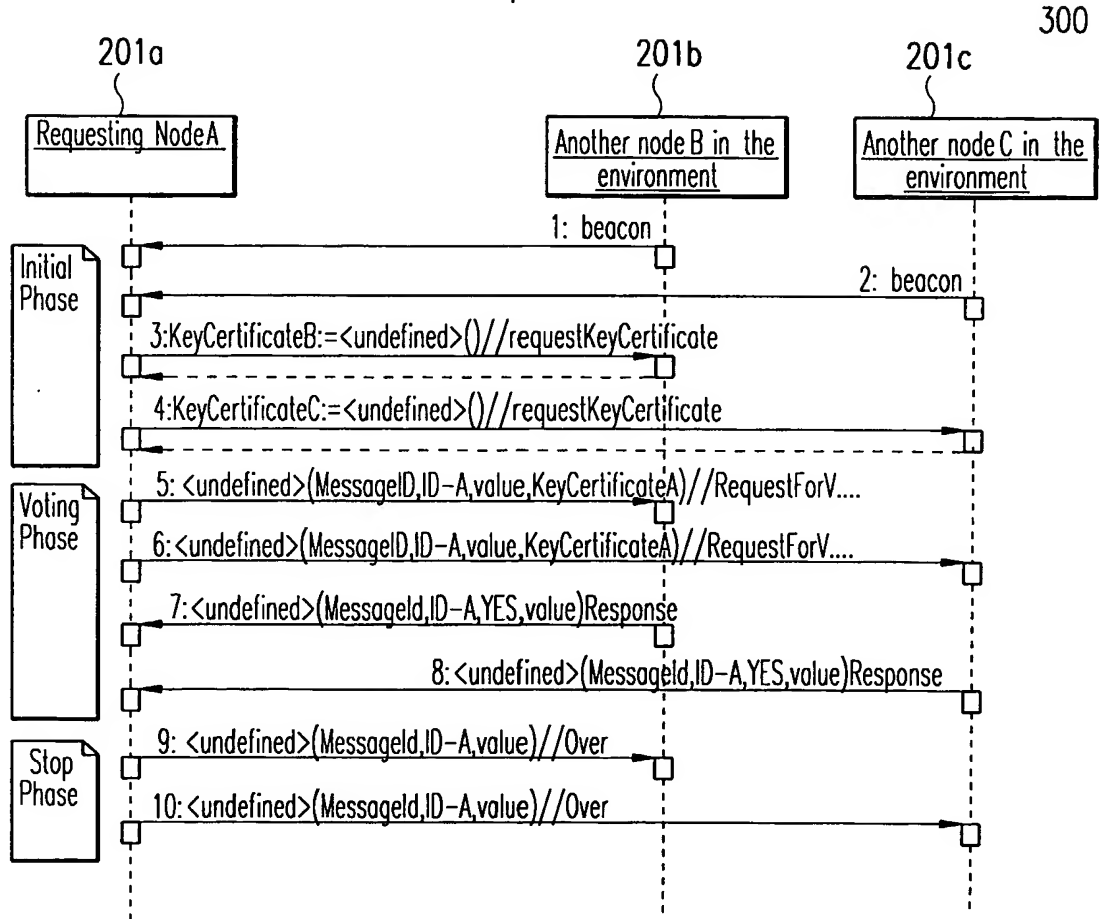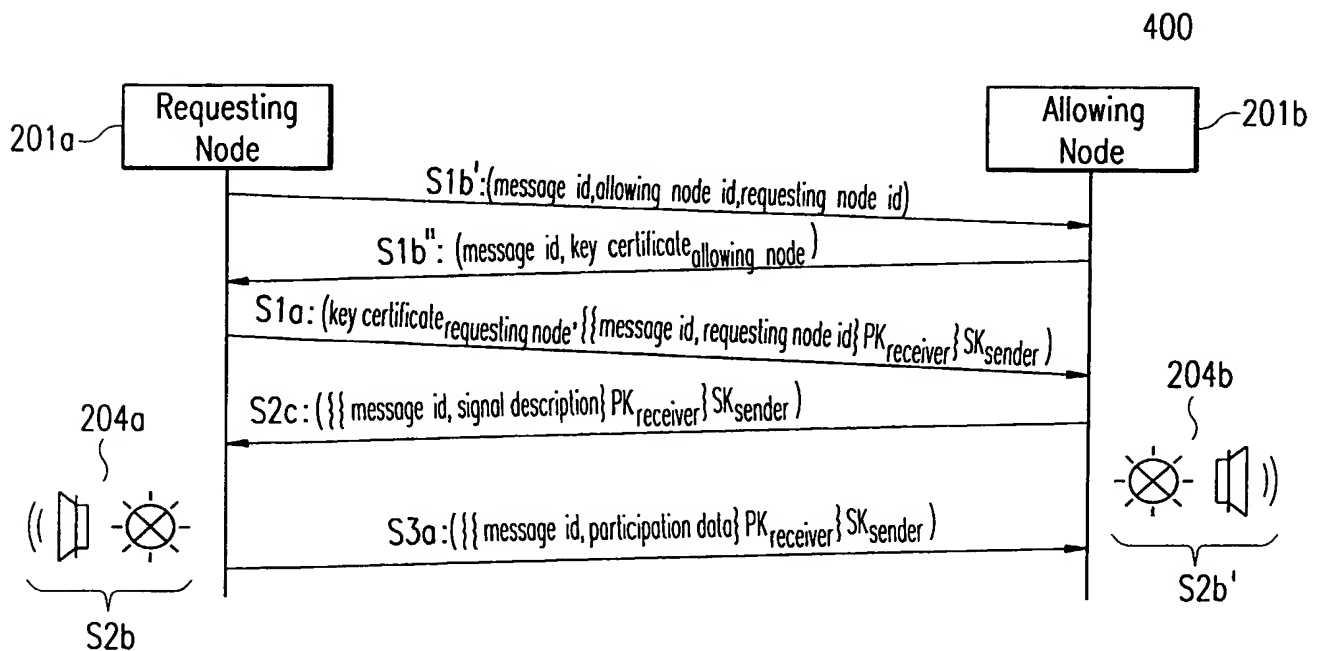
Fig. 1

Fig. 2

201a

Requesting Node A
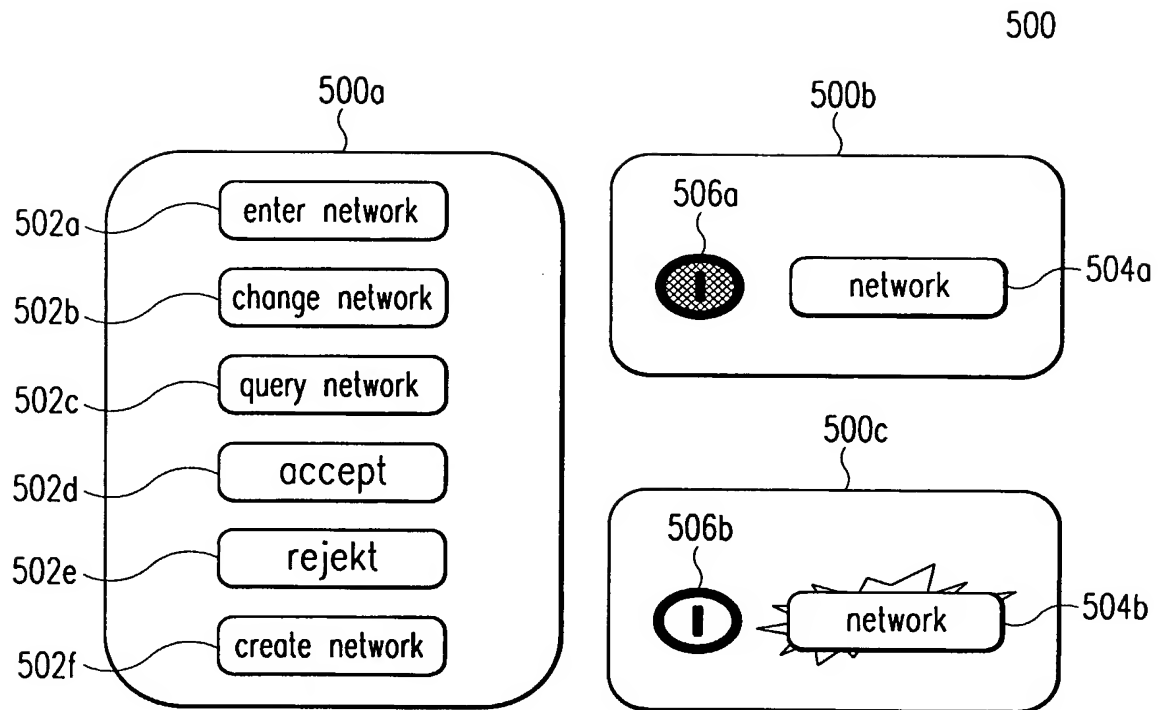
201b

Another node B in the
environment

201c

Another node C in the
environment

300

Initial Phase

1: beacon

2: beacon

3:KeyCertificateB:=<undefined>()//requestKeyCertificate

4:KeyCertificateC:=<undefined>()//requestKeyCertificate

Voting Phase

5: <undefined>(MessageID,ID-A,value,KeyCertificateA)//RequestForV....

6: <undefined>(MessageID,ID-A,value,KeyCertificateA)//RequestForV....

7: <undefined>(MessageId,ID-A,YES,value)Response

8: <undefined>(MessageId,ID-A,YES,value)Response

Stop Phase

9: <undefined>(MessageId,ID-A,value)//Over

10: <undefined>(MessageId,ID-A,value)//Over

Fig. 3

400

201a — Requesting Node

Allowing Node — 201b

$S1b'$: (message id, allowing node id, requesting node id)

$S1b''$: (message id, key certificate$_{allowing\ node}$)

$S1a$: (key certificate$_{requesting\ node}$, {{message id, requesting node id} PK$_{receiver}$} SK$_{sender}$)

$S2c$: ({{message id, signal description} PK$_{receiver}$} SK$_{sender}$)

204a

204b

$S3a$: ({{message id, participation data} PK$_{receiver}$} SK$_{sender}$)

S2b

S2b'

Fig. 4

500

500a

502a — enter network
502b — change network
502c — query network
502d — accept
502e — rejekt
502f — create network

500b

506a

network — 504a

500c

506b

network — 504b

Fig. 5